REMARKS

Amendment of Title of the Invention

Applicant requests that the title of the invention be amended to add the word "Securely" before the word -- Downloading -- , whereby the title shall read "System and Method for Securely Downloading Electronic Information to a Video Lottery Terminal".

Specification Amendments

By the present amendments of the specification applicant has corrected obvious typographical and grammatical errors and rendered some wording more concise. No new matter has been added by these amendments.

Claim Amendments

By the present amendments of claims 1 and 12 applicant has made some wording changes, as shown, to provide greater clarity and more concisely define the invention, and features recited in the preambles have been moved to the enumerated subparagraphs of the claims.

In claims 1 and 12, the wording of "at least another said key being delivered to said terminal" and "said other key" has been reordered and changed, respectively, to more clearly designate that "other" key as being the second, non-resident key (i.e. the key that is separately delivered to the terminal).

In addition, the preambles of claims 1 and 12 are amended to remove the words "through a communications link between said host device and said terminal" as being merely peripheral and unnecessary to the claimed invention. In turn, claims 3 and 14 have been amended to incorporate those words therein in conjunction with the original reference to a communications link.

In addition, claims 1 and 12 are amended, and new claims 21 and 22 are added, to provide, through those dependent claims, for the option of transmitting a next version key in the encrypted electronic information (rather than through claims 1 and 2).

Dependent claims 11 and 16 are cancelled and dependent claims 4, 12-14 and 17-19 have been amended in view of the foregoing amendments.

Applicant respectfully requests reconsideration and withdrawal of the claim rejections by the Examiner having regard to the following submissions.

35 U.S.C. §102(e) Rejection

The Examiner has indicated that claims 1-20 are rejected under 35 U.S.C. 102(e) as allegedly being anticipated by the cited reference to **Alcorn et al** (U.S. Patent No. 6,149,522).

As dictated by MPEP 706.02, in order for a patent claim to be anticipated by a cited prior art reference it must teach every aspect of the claimed invention either explicitly or impliedly and any feature not directly taught must be inherently present. With respect, applicant submits that **Alcorn et al.** do not meet this requirement with respect to any claim of this application. Moreover, as detailed in the following, the reference to **Alcorn et al.** is not directed in any respect to securing a downloading (electronic transfer) of electronic information from a host to a client and, instead, pertains to subject matter unrelated to applicant's invention.

As its title and description show, the **Alcorn et al.** reference discloses means for authenticating a given collection of data sets to make sure they haven't been tampered with prior to their execution by a game console (i.e. prior to a player playing the game), not for securing the delivery of those game data sets, themselves, so that they are authentic when stored for execution by the game console. As detailed at column 2,

lines 10-34, **Alcorn et al.** seek to overcome the disadvantage of prior art authentication means whereby game data sets were stored on unalterable ROM and those data sets were authenticated by physically removing the ROM and comparing content of the ROM to that of a custodial version of the data sets maintained by a secure authority. The need for storing the game data sets on unalterable ROM, and for physically handling that ROM in the authentication process, were found to be too restrictive with the increased size, number and types of storage required by modern game data sets. **Alcorn et al.** provide an alternative to that prior art whereby the data sets are stored without restriction on read/write storage and are authenticated by software means within the game console (i.e. no physical removal of the game data). Instead of maintaining the data sets themselves on unalterable ROM, **Alcorn et al.** maintain authentication data sets on unalterable ROM (the idea being that the storage requirements of these data sets do not expand and vary as much as those for the game data sets and, so, external authentication of those authentication data sets can be done according to the prior art with greater convenience).

By the method of **Alcorn et al.** the game data sets are stored in suitable (unrestricted) storage for use by the gaming console to play the game. In addition, that storage includes, with the game data sets, an encrypted signature that is calculated from the game data sets. Separate from that unrestricted storage, is unalterable ROM containing authentication software (data sets) for calculating a check signature from the stored game data sets (i.e. using the same hash function calculations as those used to calculate the encrypted signature), together with the signature for those game data sets and the decryption code (means) for decrypting the encrypted signature on the unrestricted storage. To authenticate the game data sets in the unrestricted storage, the authentication software is run on them and their signature is calculated using the authentication software and compared to the decrypted signature calculated by decrypting the encrypted signature using the ROM-stored decryption code.

In a more complex embodiment, referred to by **Alcorn et al.** as a "two-stage" method of authenticating game data sets, they provide a further, optional, layer of similar authentication means whereby two separate authentication software applications are run. A first authentication program stored in a first storage means is first used to authenticate a second, separately stored authentication application referred to as "an anchor application" and, if that anchor application is found to be valid, it is used to authenticate the game data sets as described by the foregoing (see column 5, lines15-61 and column 11, lines 3-67).

By contrast to **Alcorn et al.**'s foregoing method of data authentication, the applicant provides a method securing data transfer and the timing, purpose and character of this method are all very different and unrelated. The applicant's data transfer securing method is applied at a much earlier stage of data handling, namely, at the time data is transferred from a host to a client rather than much later on, per **Alcorn et al.**, when a fixed set of already captured data is checked to verify, as against a master reference, that it is authentic (unaltered over that master reference). The applicant's data transfer securing method is for the purpose of securing data so that it is secure and that security is maintained for a transfer of the data to a client and decryption of the data by that client i.e. to ensure that the data held by the host is the same as that captured and decrypted by a client and no unauthorized access and alteration of the data occurs in the interim. By contrast, the purpose of **Alcorn et al.**'s data authentication method is to check data that is already held by a client, by comparing it against a master reference, to ensure the data has not been corrupted or altered while held by the client. As such, the character and components of each method/system are both very different and uncomparable.

The following two fundamental distinctions exist between applicant's claimed system (claim 1) and method (claim 12) and those of **Alcorn et al.**'s system and method:

1. In applicant's system and method, each and every byte/bit of the electronic information (data) that is transferred from a host to a client is secured by encryption of the entirety of that information (data), whereas **Alcorn et al.** do not secure any data at all. Rather, they simply use the data to calculate a separate, short (several bits only) electronic signature and no change is made to the data itself. Unlike **Alcorn et al.**, in applicant's system the entirety of that secured data replaces the electronic information stored in the terminal, that is, by enabling a replacement of the stored information with corresponding decrypted information obtained from decrypting the encrypted information; and,

2. Applicant's system and method secure the data by means encrypting it using two encryption keys before it is transferred, one key being held by the terminal (client) but the other, non-resident key being maintained separate from the terminal and separately provided to the terminal apart from the encrypted information. Both of these separately-maintained keys are required, and used, by the terminal to decrypt the data once it is received by the terminal.

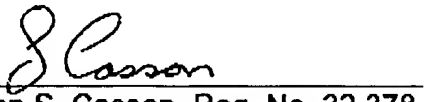
Applicant submits that the foregoing different features of the invention clearly demonstrate that the cited reference to Alcorn et al. does not anticipate any claim of this application. Further, applicant submits that the claimed invention cannot be considered to be obvious over **Alcorn et al.**, or over **Alcorn et al.** in view of any prior art, because **Alcorn et al.** disclose subject matter unrelated to applicant's method and system.

CONCLUSIONS

For all the foregoing reasons, applicant respectfully submits that claims 1-22 as amended and pending in this application are in good order and ready for allowance. Reconsideration of the Office Action and an early Notice of Allowance are respectfully requested. In the event that the Examiner cannot allow the present application for any

reason, the Examiner is encouraged to contact applicant's attorney to discuss resolution of any remaining issues.

Respectfully Submitted,
GORDON

By: 
Lynn S. Cassan, Reg. No. 32,378
(Agent appointed by Applicant)

Cassan Maclean
401 - 80 Aberdeen St.
Ottawa, Ontario
K1S 5R5
Phone: 613-238-6404

Date: November 8, 2004